SIRI & GLIMSTAD LLP
Kyle McLean (SBN 330580)
E: kmclean@sirillp.com
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 376-3739
Fax: (646) 417-5967

Mason A. Barney (*pro hac vice* to be filed)
E: mbarney@sirillp.com
Steven D. Cohen (*pro hac vice* to be filed)
E: scohen@sirillp.com
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
Fax: (646) 417-5967

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

SERGIO ORTEGA and LEQUEINT COLE, on behalf of themselves and all others similarly situated, Plaintiffs, v. HERITAGE PROVIDER NETWORK, INC., REGAL MEDICAL GROUP, INC., LAKESIDE MEDICAL ORGANIZATION, A MEDICAL GROUP, INC., ADOC ACQUISITION CO., A MEDICAL GROUP, INC., GREATER COVINA MEDICAL GROUP INC., ARIZONA HEALTH ADVANTAGE, INC. d/b/a ARIZONA PRIORITY CARE, AND AZPC CLINICS, LLC, Defendants.	Case No. 23-cv-331 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Sergio Ortega and Lequeint Cole, individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiffs"), allege the

following against Heritage Provider Network, Inc. ("HPN"), Regal Medical Group, Inc. ("Regal"), Lakeside Medical Organization, A Medical Group Inc. ("Lakeside"), ADOC Acquisition Co., A Medical Group, Inc. ("ADOC"), Greater Covina Medical Group Inc. ("Covina"), Arizona Health Advantage Inc. d/b/a Arizona Priority Care ("APC"), and AZPC Clinics, LLC ("AZPC") (collectively "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiffs brings this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly-situated patients' names, Social Security numbers, dates of birth, addresses, medical diagnoses and treatment, treatment dates and information, phone numbers, service authorization numbers, health plan numbers, and other sensitive medical records from hackers.

2. HPN, based in Southern California, is a healthcare network that serves California patients. HPN is one of the largest private healthcare networks in the U.S. Defendants Regal, Lakeside, ADOC, Covina, APC, and AZPC are all part of HPN.

3. On or about February 3, 2023, Regal sent out data breach letters ("Data Breach Notice" or "Notice") to individuals whose information was compromised as a result of what it referred to as "a ransomware cyberattack." Regal reported that the attack was on its systems as well as on the systems of other HPN subsidiaries Lakeside, ADOC, and Covina. On information and belief, APC sent out its own data breach letters to impacted individuals.

4. Based on the Notices sent by Regal and APC and news reports, on December 2, 2022, Defendants "noticed difficulty in accessing some of [their] servers." In response, Defendants claim that they performed a review. That review revealed that malware was present on some of their servers and that an unauthorized

party had accessed and exfiltrated certain files (the "Data Breach"). The Data Breach impacted HPN, Regal, Lakeside, ADOC, Covina, APC, and AZPC.

5. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes names, Social Security numbers, dates of birth, addresses, medical diagnoses and treatment, treatment dates and information, phone numbers, service authorization numbers, health plan numbers, and other sensitive medical records (collectively, the "Private Information") and includes personally identifiable information ("PII") and protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") that Defendants collected and maintained.

6. Armed with the Private Information accessed in the Data Breach and a head start, a data thief could commit a variety of crimes including, *e.g.*, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, and filing fraudulent tax returns using Class Members' information.

7. Plaintiffs and Class Members have thus suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

8. Plaintiffs brings this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained.

9. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the Private Information left that Private Information vulnerable to an attack.

10. Upon information and belief, Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. If Defendants had properly monitored their networks, they would have discovered the Data Breach sooner than they did.

11. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct, as the Private Information, PII, and PHI that Defendants collected and maintained is now likely in the hands of data thieves and unauthorized third-parties.

12. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

13. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

14. Plaintiff Sergio Ortega is, and at all times mentioned herein was, an individual citizen of the State of California residing in the City of Corona in Riverside County.

15. Plaintiff Lequeint Cole is, and at all times mentioned herein was, an individual citizen of the State of Arizona residing in the City of San Tan Valley in Pinal County.

16. Defendant HPN is a healthcare network with locations across southern California and with its central location in Northridge, California in Los Angeles County. HPN is incorporated in California. HPN administers health care groups, including Defendants Regal, ADOC, Lakeside, Covina, APC, and AZPC.

17. Defendant Regal is a healthcare provider with various locations in Southern California. Regal is affiliated with Lakeside, ADOC, and Covina. Regal issued the Data Breach Notice on behalf of itself, Lakeside, ADOC, and Covina. Regal is incorporated in California. Regal is a subsidiary of HPN.

18. Defendant Lakeside is a healthcare provider with its principal place of business in Burbank, California and is incorporated in California. Lakeside is a subsidiary of HPN.

19. Defendant ADOC is a healthcare provider with its principal place of business in Northridge, California and is incorporated in California. ADOC is a subsidiary of HPN.

20. Defendant Covina is a healthcare provider with its principal place of business in Northridge, California and is incorporated in California. Covina is a subsidiary of HPN.

21. Defendant APC is a healthcare provider with its principal place of business in Chandler, Arizona. APC is a subsidiary of HPN.

22. Defendant AZPC is a healthcare provider with its principal place of business in Chandler, Arizona. AZPC is a subsidiary of HPN.

JURISDICTION AND VENUE

23. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is well over 100, some of whom have different citizenship than one or more Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has jurisdiction over Defendants because HPN operates in and has its principal place of business in this District where it provides administration services for each of the other subsidiary Defendants.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendants have harmed Class Members residing in this District.

HPN COLLECTS HIGHLY SENSITIVE INFORMATION

26. Founded in 1979, HPN is a healthcare network based in Southern California. HPN is comprised of over 3,700 primary care physicians, over 10,000 specialists and almost 1,700 affiliated facilities. HPN is one of the largest network providers in California. HPN is estimated to have an annual revenue approaching $700 million. HPN administers multiple medical groups, including the following:

a. Defendant Regal
b. Defendant Lakeside
c. Defendant ADOC
d. Defendant Covina
e. Defendant APC
f. Defendant AZPC
g. Bakersfield Family Medical Center
h. Coastal Communities Physician Network
i. Desert Oasis Health Care
j. High Desert Medical Group
k. Heritage Victor Valley Medical Group
l. Sierra Medical Group

27. As a condition of receiving medical services, Defendants require that their patients entrust them with highly sensitive PII and PHI. In the ordinary course of receiving services, patients are required to provide sensitive personal and private information such as names, Social Security numbers, dates of birth, addresses, phone numbers, and sensitive medical and health insurance information, among other things.

28. In its Privacy Policy, Defendant Regal promises patients that it "has adopted and adheres to stringent security standards designed to protect non-public personal information … against accidental or unauthorized access or disclosure."[1] Regal also describes in its Privacy Policy the limited, specific instances when Regal shares patient health information and says that it will not share patients' information "other than described here unless you tell us we can in writing."[2] Regal explains on its website that it does so in order to comply with HIPAA.[3] Pursuant to its privacy notice mandated by HIPAA, Regal explains to its patients that it is "required by law to maintain the privacy and security of your protected health information" and that it "will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[4]

29. HPN's HIPAA Notice of Privacy Practice makes similar promises, including that it is "required by law to maintain the privacy and security of your protected health information," that it "must follow the duties and privacy practices described in this notice," and that it "will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[5] On

---

[1] *See* Regal Notice of Privacy Practices, www.regalmed.com/privacy-notice/ (last visited Feb. 24, 2023).

[2] *See* Regal Notice of Privacy Practice, www.regalmed.com/Regal-en-us/assets/File/RMG-Notice-of-Privacy-Practice.pdf (last visited Feb. 24, 2023).

[3] *See* Regal Notice of Privacy Practices, www.regalmed.com/privacy-notice/ (last visited Feb. 24, 2023).

[4] *See* Regal Notice of Privacy Practice, www.regalmed.com/Regal-en-us/assets/File/RMG-Notice-of-Privacy-Practice.pdf (last visited Feb. 24, 2023).

[5] *See* Heritage Provider Network Notice of Privacy Practice, https://www.heritageprovidernetwork.com/files/Privacy%20Practice.pdf (last visited Feb. 24, 2023).

information and belief, HPN's HIPAA Notice of Privacy Practice or an essentially identical notice is provided to patients of all Defendants.

30. APC's Notice of Privacy assures patients that:

> Uses and disclosures of your protected health information that involve the release of psychotherapy notes (if any), marketing, sale of your protected health information, or other uses and disclosures not described in this notice or required by law will be made only with your separate written permission.[6]

31. On information and belief, other Defendants have the same or similar privacy policies as Regal, HPN, and APC.

32. On information and belief, Defendants provide each of their patients with a copy of their Privacy Policy and require each to sign an acknowledgment with regard to the Privacy Policy.

33. Defendants use Private Information from patients to provide medical and healthcare-related services to patients.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

35. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

36. Plaintiffs and Class Members relied on Defendants to keep their Private Information, PII, and PHI confidential and securely maintained and to only make authorized disclosures of this information.

[6] *See* APC Notice of Privacy, https://azprioritycare.com/wp-content/uploads/2020/07/AZPC-Notice-Of-Privacy-Practices.pdf (last visited Feb. 24, 2023).

HPN'S DATA BREACH AND NOTICE

37. Plaintiff Ortega was a patient of Regal and therefore also HPN. As part of receiving medical services from Regal, Regal collected, *inter alia*, Plaintiffs' name, date of birth, Social Security number, address, phone number, and medical and health insurance information.

38. Plaintiff Cole was a patient of APC and therefore also HPN. As part of receiving medical services from APC, APC collected, *inter alia*, Plaintiffs' name, date of birth, Social Security number, address, phone number, and medical and health insurance information.

39. According to Regal and APC, in early December 2022, Regal and APC learned of unauthorized access that occurred on or about December 1, 2022 to computer systems of Regal, Lakeside, ADOC, Covina, APC, and AZPC, all of which are entities administered by HPN. Both Regal and APC indicate that Regal and APC employees "noticed difficulty in accessing some of our servers." APC says that it "became aware" of the Data Breach on December 5, 2022 while Regal says that it "became aware" of the Data Breach on December 8, 2022.

40. The Regal notices indicates that as part of "a ransomware cyberattack," an unauthorized individual or individuals accessed a cache of highly sensitive PII and PHI, including patient names, dates of birth, Social Security numbers, addresses, phone numbers, and medical and health insurance information. The APC refers to the breach as involving malware and identifies the same or similar information as being "impacted personal information."

41. On or about February 3, 2023, two months after first learning of the Data Breach, Defendants began to notify their patients that its investigation had identified that their Private Information, PII, and PHI had been breached. The Data Breach Notification Letter sent to Plaintiff Ortega stated that "we believe that your personal information may have been impacted in the incident, and that your

impacted personal information may include your name, social security number . . . , date of birth, address, diagnosis and treatment, laboratory test results, prescription data, radiology reports, health plan member number, and phone number."

42. The Data Breach Notification Letter continued with sections entitled "What We Are Doing," "What You Can Do," "Other Information," and "For More Information." Other than offering one year of credit monitoring so long as victims affirmatively call and request it,[7] recommending that victims register fraud alerts with credit bureaus and order credit reports, and providing a phone number that victims could call if they "have any additional questions about this incident," Defendants offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves, including with regard to their health, medical, and insurance information.

43. On information and belief, Defendants sent a similar generic letter to all individuals affected by the Data Breach.

44. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Class Members' Private Information, PII, and PHI confidential and to protect from unauthorized access and disclosure.

45. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

[7] Notably, Defendants' offer to provide only one year of credit monitoring is buried in the Data Breach Notification Letter such that many patients are unlikely to realize that is being offered. Additionally, on information and belief, it may be difficult for patients to locate the referenced phone number that they need to call to receive credit monitoring services.

46. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks, especially in the healthcare industry.

47. Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

DATA BREACHES IN HEALTHCARE AND THE DISRUPTION THEY CAUSE

48. According to the Ponemon Institute and Verizon Data Breach Investigations Report, the health industry experiences more data breaches than any other sector.[8] Regular PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] However, PHI can sell for as much as $363 according to the Infosec Institute.[10] This is because one's personal health history cannot be changed unlike credit card information.

49. PHI has increased value because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale.

---

[8] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Feb. 24, 2023).

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 24, 2023).

[10] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Feb. 24, 2023).

50. Because of the value of its data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries. This is well known in the healthcare industry.

51. Cyberattacks and data breaches at healthcare providers are especially problematic because they can negatively impact the overall daily lives of patients affected by the attack.

52. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the incident.[11] Researchers have also found that at medical service providers that experienced a data security incident, the incident was associated with an overall deterioration in timeliness and patient outcomes.[12]

DEFENDANTS FAILED TO COMPLY WITH FTC GUIDELINES

53. The Federal Trade Commission (the "FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer

[11] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptickin-fatal-heart-attacks (last visited Feb. 24, 2023).

[12] *See* Sung J. Choi, *et al.*, *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Feb. 24, 2023)

needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against entities for failing to adequately and reasonably protect data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. On information and belief, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

58. Defendants were at all times fully aware of their obligation to protect the PII and PHI of their patients.

59. Defendants knew or should have known of the risks they faced as medical service providers and should have strengthened their data systems

accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach yet they failed to properly prepare for that risk.

HPN FAILED TO COMPLY WITH INDUSTRY STANDARDS

60. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

61. Some industry best practices that should be implemented by entities like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. Upon information and belief, Defendants failed to follow some or all of these industry best practices.

62. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. Upon information and belief, Defendants failed to follow these cybersecurity best practices, including failure to train their staff.

63. Upon information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), the HIPAA Security Rule and Breach Notification Rule, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity

readiness. Defendants' failure to comply with these accepted standards opened the door to the cyber incident resulting in the Data Breach.

DEFENDANTS' SECURITY OBLIGATIONS AND VIOLATIONS OF HIPAA

64. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data.

65. HIPAA requires covered entities like Defendants to protect against reasonably anticipated threats to the security of sensitive patient health information. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling the types of data that Defendant left unguarded. The HHS subsequently promulgated multiple regulations.

67. Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.10.

68. On information and belief, Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect their patients' Private Information;

c. Failing to properly monitor their data security systems for existing intrusions;

d. Failing to sufficiently train their employees regarding the proper handling of PII and PHI;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of Section 5 of the FTCA;

f. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(4);

g. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption"); and

h. Failing to adhere to industry standards for cybersecurity.

69. On information and belief, as a result of computer systems in need of security upgrades, inadequate procedures for handling emails containing viruses or other malignant computer code, and/or employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

70. On information and belief, the Data Breach resulted from a combination of insufficiencies that demonstrate that Defendants failed to comply with safeguards mandated by HIPAA regulations.

71. Accordingly, as outlined below, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they now face an increased risk of fraud and

identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants.

DATA BREACHES, FRAUD, AND IDENTITY THEFT

72. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[13] Exposure of personal information that a consumer wishes to keep private may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

73. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited Feb. 24, 2023).

personal information through means such as spam phone calls and text messages or phishing emails.

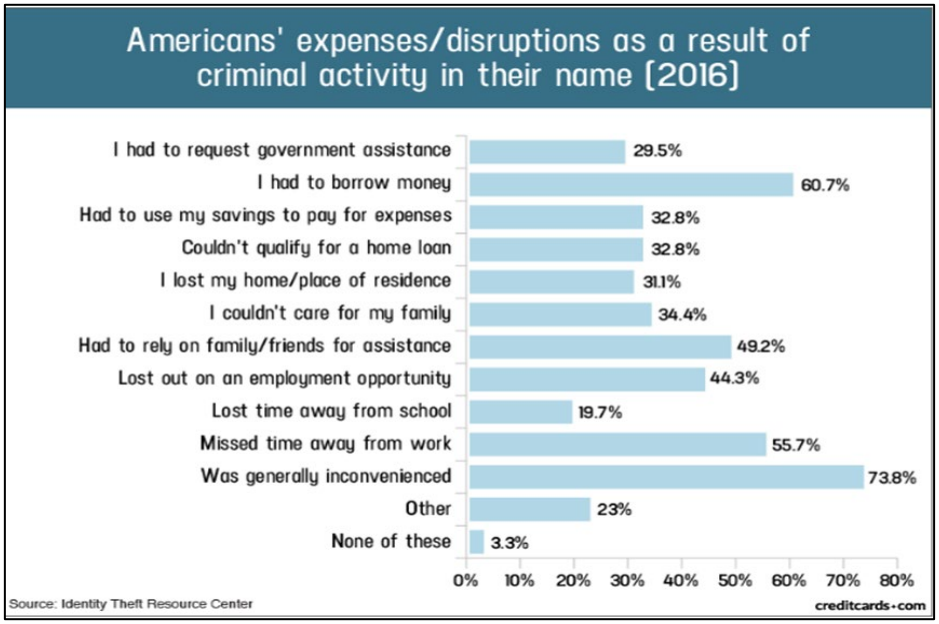
74. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14]

75. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

76. Identity thieves can also use Social Security numbers to obtain an official identification card in the victim's name but with the thief's picture, use the victim's name and Social Security number to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[14] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Feb. 24, 2023).

77. A study by the Identity Theft Resource Center[15] shows the multitude of harms caused by fraudulent use of PII:



78. Moreover, the value of Private Information is axiomatic. The value of "big data" in corporate America is astronomical. Meanwhile, the consequences of cyberthefts include heavy prison sentences. The fact that identity thieves attempt to steal identities notwithstanding these possible heavy prison sentences illustrates beyond a doubt that Private Information has considerable market value.

79. Theft of medical-related PHI is particularly troubling and can result in medical identity theft, where a thief uses the victim's information to see a doctor, get prescription drugs, buy medical devices, submit insurance claims, or get other medical care.[16] If the thief's health information is mixed with the victim's health

[15] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Feb. 24, 2023).

[16] *What To Know About Medical Identity Theft*, Federal Trade Commission (May 2021), *available at* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Feb. 24, 2023).

information, that could negatively impact the victim's health insurance benefits and credit.

80. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of marketing their products and services to the physical maladies of the data breach victims themselves. Some insurance companies purchase and use wrongfully-disclosed PHI to adjust their insureds' medical insurance premiums.

81. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[17]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

82. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

[17] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Feb. 21, 2023).

83. As a result, there is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning that Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

84. Plaintiffs and Class Members have been damaged by the compromise of their Private Information, PII, and PHI in the Data Breach.

85. Plaintiffs' Private Information, including sensitive PII and PHI, was compromised as a direct and proximate result of the Data Breach.

86. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

87. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

88. Plaintiffs and Class Members face a substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, medical fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

89. Plaintiffs and Class Members face a substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information, as potential fraudsters could use that information to target their schemes more effectively to Plaintiffs and Class Members.

90. Plaintiffs and Class Members also face substantial risk of being victims of medical identity theft.

91. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

92. The information that Defendants maintain regarding Plaintiffs and Class Members combined with publicly available information allows nefarious actors to assemble a detailed picture of Plaintiffs and Class Members.

93. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages.

94. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their accounts and records for misuse.

95. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered of will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;
b. Canceling and reissuing credit and debit cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Placing "freezes" and "alerts" with credit reporting agencies;
e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
f. Contacting financial institutions and closing or modifying financial accounts; and
g. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

96. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security

measures and safeguards, including but not limited to making sure that the storage of data or documents containing personal information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

97. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and either have suffered harm or are at an increased risk of future harm.

CLASS ALLEGATIONS

98. Plaintiffs brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and on behalf of all other persons similarly situated (the "Class").

99. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

California Subclass

All residents of California who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Arizona Subclass

All residents of Arizona who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

100. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

101. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

102. Each of the proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

103. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Based on Defendants' reporting to HHS, the Class consists of **more than 3.3 million** HPN-affiliated patients whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

104. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;
b. Whether Defendants' conduct violated the California Consumer Privacy Act ("CCPA") invoked below;
c. Whether Defendants' conduct violated California's Unfair Competition Law ("UCL") invoked below;
d. Whether Defendants' conduct violated California's Confidentiality of Medical Information Act ("CMIA") invoked below;
e. Whether Defendants' conduct violated California's Consumers Legal Remedies Act ("CLRA") invoked below;

f. Whether Defendants' conduct violated the Arizona Consumer Fraud Act ("ACFA") invoked below;

g. When Defendants actually learned of the Data Breach and whether their response was adequate;

h. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

i. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

k. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

l. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

m. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

n. Whether hackers obtained Class Members' Private Information via the Data Breach;

o. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

p. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

q. Whether Defendants' conduct was negligent;

r. Whether Defendants' conduct was *per se* negligent;

s. Whether Defendants were unjustly enriched;

t. Whether Defendants breached their fiduciary duties to Plaintiffs and Class Members;

u. Whether Defendants violated Plaintiffs' and Class Members' privacy interests;

v. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

w. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

x. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

105. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

106. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

107. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that, upon information and belief, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

108. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common

questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

109. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted or have refused to act on grounds generally applicable to the Class so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

110. Finally, all members of the proposed Class are readily ascertainable. On information and belief, Defendants have access to the names, addresses, and emails of all Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

111. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

112. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, PII, and PHI, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such

information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

113. Defendants knew or should have known of the risks inherent in collecting the Private Information, PII, and PHI of Plaintiffs and Class Members and the importance of adequate security. Defendants were on notice because they knew or should have known that they would be an attractive target for cyberattacks, especially as a healthcare provider.

114. Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them as a result of the special relationship between Defendants and their patients, recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information, PII, and PHI in their possession;

b. To protect Private Information, PII, and PHI using reasonable and adequate security procedures and systems that are compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information, PII, and PHI in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information, PII, and PHI of Plaintiffs and Class Members pursuant to the FTCA, CCPA, UCL, CMIA, CLRA, ACFA, and HIPAA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the types of information compromised.

115. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

116. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants were bound by industry standards to protect confidential Private Information.

117. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm. It was reasonably foreseeable that Defendants' failure to utilize adequate security measures to protect Class Members' Private Information would result in injury to Class Members. The Data Breach was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

118. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information, PII, and PHI within Defendants' possession.

119. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information, PII, and PHI of Plaintiffs and Class Members.

120. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information, PII, and PHI. On information and belief, the specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information, PII, and PHI;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system maintained reasonable data security safeguards; and

d. Allowing unauthorized access to Class Members' Private Information, PII, and PHI.

121. Plaintiffs' and Class Members' willingness to entrust Defendants with their Private Information, PII, and PHI was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Private Information that they stored there) from attack.

122. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information, PII, and PHI to be compromised.

123. Defendants' breaches of duty caused a foreseeable risk to Plaintiffs and Class Members that they would be harmed by suffering from identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

124. As a result of Defendants' negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

125. Defendants also had independent duties under California and Arizona state law (including the CCPA and ACFA) that required them to reasonably safeguard Plaintiffs' and Class Members' Private Information, PII, and PHI.

126. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of further harm.

127. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

128. The injury and harm that Plaintiffs and Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

129. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

130. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, inter alia, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

131. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

132. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard Plaintiffs' and Class Members' Private Information, PII, and PHI.

133. Pursuant to HIPAA, Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PHI.

134. Under HIPAA, Defendants had a duty to render electronic PHI into unusable, unreadable, or indecipherable form. *See* 45 C.F.R. § 164.304.

135. Defendants breached their duties by, upon information and belief, failing to employ industry-standard cybersecurity measures in order to comply with the FTCA and their obligations under HIPAA, including but not limited to: proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

136. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect.

137. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information. The FTC publications described above and the industry-standard cybersecurity measures also form part of the basis of Defendants' duty in this regard.

138. Defendants violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards.

139. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information in the medical industry, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information, PII, and PHI in compliance with applicable laws would result in an unauthorized

third party gaining access to Defendants' networks, databases, and computers that stored or contained Plaintiffs' and Class Members' Private Information.

140. Defendants' violations of the FTCA and HIPAA constitute negligence *per se*.

141. Plaintiffs' and Class Members' Private Information, PII, and PHI constitute personal property that was stolen due to Defendants' negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

142. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information (including PII and PHI) because of the Data Breach, including but not limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

143. Defendants breached their duties to Plaintiffs and the Class under FTCA and HIPAA, as well as under California and Arizona state laws (discussed below) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information, PII, and PHI.

144. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

145. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

146. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

147. Plaintiffs and Class Members entered into a valid and enforceable contract through which Defendants provided services to Plaintiffs and Class Members. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

148. Defendants' Privacy Policy memorialized the rights and obligations of Defendants and their patients. In its Privacy Policy, Defendants commits to protecting the privacy and security of personal information and promises to never share such information except under certain limited defined circumstances.

149. Defendants promised to comply with all HIPAA standards, state and federal law, to ensure Plaintiffs' and Class Members' PHI was protected, secured, kept private, and not disclosed, and to promptly notify Plaintiffs and Class Members of any data breach.

150. Plaintiffs and Class Members fully performed their obligations under their contracts with Defendants.

151. However, Defendants did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' PII and PHI, and therefore Defendants breached their contract with Plaintiffs and Class Members.

152. Defendants allowed third parties to access, copy, and/or transfer Plaintiffs' and Class Members' PII and PHI without permission. Therefore, Defendants breached the Privacy Policy with Plaintiffs and Class Members.

153. Defendants' failure to satisfy its confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs and Class Members that were of a diminished value.

154. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein.

155. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

156. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

157. This Count is pleaded in the alternative to Count III above.

158. Defendants provide medical services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendants regarding the provision of those services through their collective conduct.

159. Through Defendants' provision of services, they knew or should have known that they must protect Plaintiffs' and Class Members' confidential Private Information, PII, and PHI in accordance with Defendants' policies, practices, and applicable law, including the FTCA, CCPA, UCL, CLRA, CMIA, ACFA, and HIPAA.

160. As part of receiving services, Plaintiffs and Class Members turned over valuable PII and PHI to Defendants. Accordingly, Plaintiffs and Class Members bargained with Defendants to securely maintain and store their Private Information.

161. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

162. Plaintiffs and Class Members have been damaged by Defendants' conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

163. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

164. In light of the special relationship between Defendants and Plaintiffs and Class Members whereby Defendants became guardian of Plaintiffs' and Class Members' Private Information, Defendants became a fiduciary to act primarily for Plaintiffs and Class Members for the safeguarding of Plaintiffs' and Class Members' Private Information, to timely notify Plaintiffs and Class Members of a data breach, and to maintain complete and accurate records of the personal information that Defendants maintain.

165. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to safeguard and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

166. Defendants also breached their fiduciary duties to Plaintiffs by failing to promptly notify Plaintiffs and Class Members of the Data Breach.

167. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with

the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of Plaintiffs' and Class Members' lives; and (vii) the diminished value of Defendants' services.

168. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
VIOLATION OF THE CCPA, CAL. CIV. CODE § 1798, *ET SEQ.* (ON BEHALF OF PLAINTIFF ORTEGA AND THE CALIFORNIA SUBCLASS)

169. Plaintiff Ortega restates and realleges the allegations in paragraphs 1-110 as if fully set forth herein.

170. As fully alleged above, Defendants HPN, Regal, Lakeside, ADOC, and Covina (the "California Defendants") engaged in unfair and deceptive acts and practices in violation of the CCPA.

171. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and

maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

172. The California Defendants are subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

173. Additionally, earlier this year, the CCPA was amended to provide new rights to consumers including the right to limit the use and disclosure of sensitive personal information collected for them. The California Defendants failed to comply with this as well.

174. Section 1798.100(e) of the CCPA states: "A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure . . . ."

175. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

176. Plaintiff Ortega is a "consumer" as defined by Cal. Civ. Code § 1798.140(g) because he is a natural person residing in the state of California.

177. The California Defendants meet the definition of a "business" as defined by Civ. Code § 1798.140(c) because they are corporations that do business in the state of California and have total annual revenues of in excess of $25,000,000.

178. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination

with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (i) Social security number[;] (ii) Driver's license number[;] . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Cal. Civ. Code § 1798.150(a)(1); Cal. Civ. Code § 1798.81.5(d)(1)(A). The Data Breach included "personal information" within the meaning of the CCPA.

179. Through the Data Breach, Plaintiff Ortega's and California Subclass Members' Private Information was accessed without authorization, exfiltrated, and stolen in a nonencrypted and/or nonredacted format.

180. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

181. Additionally, Cal. Civ. Code § 1798.82 requires that any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery of notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. . . . in the most expedient time possible and without unreasonable delay . . . ." As discussed above, the California Defendants waited two months to notify Plaintiff of the breach. The California Defendants violated this provision as a result.

182. Plaintiff Ortega has sent written notice to the California Defendants pursuant to Cal. Civ. Code § 1798.150(b)(1) identifying the specific provisions of the CCPA Plaintiff Ortega alleges they have violated or are violating. Although a cure is not possible under the circumstances, if (as expected) the California Defendants are unable to cure or do not cure the violations within 30 days of Plaintiff

Ortega's letters, Plaintiff Ortega will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

183. As a result of the California Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek actual pecuniary damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII
VIOLATION OF THE UCL, CAL. BUS. PROF. CODE § 17200, *ET SEQ.* (ON BEHALF OF PLAINTIFF ORTEGA AND THE CALIFORNIA SUBCLASS)

184. Plaintiff Ortega restates and realleges the allegations in paragraphs 1-110 as if fully set forth herein.

185. Defendants violated the UCL, Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard California Subclass Members' Private Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they would and did comply with the requirement of relevant federal and state laws relating to privacy and security of California Subclass Members' Private Information; omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information; and collecting California Subclass Members' Private Information without adequately protecting or storing their Private Information.

186. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, California Subclass Members were injured and lost money or property, including but not limited to, overpayments that Defendants received to

maintain adequate security measures but did not, the loss of their legally protected interest in the confidentiality and privacy of their Private Information, PII, and PHI, and additional losses described above.

187. Defendants knew or should have known that their administrative and data security measures were inadequate to safeguard California Subclass Members' Private Information and that the risk of a data breach or unauthorized access was likely. Defendant had the resources to secure and/or prepare for protecting its patients' Private Information, PII, and PHI in a data breach. Defendant's actions in engaging in the above unfair, unlawful, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to Plaintiffs' and Class Members' rights.

188. Plaintiffs seeks relief under the UCL, including restitution to Plaintiffs and Class Members of money or property that Defendants may have acquired by means of their deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. § 1021.5), and injunctive or other equitable relief.

189. Defendants did not inform their patients that they failed to properly safeguard their Private Information, PII, and PHI thus misleading California Subclass Members in violation of § 17200, *et seq*. Such misrepresentation was material because California Subclass Members entrusted Defendants with their Private Information, PII, and PHI.

190. Had California Subclass Members known of Defendants' failure to maintain adequate security measures to protect their Private Information, California Subclass Members would not have entrusted their Private Information, PII, and PHI to Defendants.

191. California Subclass Members were injured because: (a) they would not have paid for services from Defendant had they known the true nature and character

of Defendant's data security practices; (b) California Subclass Members would not have entrusted their Private Information to Defendants in the absence of promises that Defendants would keep their information reasonably secure; and (c) California Subclass Members would not have entrusted their Private Information to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

192. As a result, California Subclass Members have been damaged in an amount to be proven at trial.

193. On behalf of himself and other California Subclass Members, Plaintiff Ortega seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages, treble damages, and reasonable attorneys' fees.

COUNT VIII
VIOLATION OF THE CMIA, CAL. CIV. CODE § 56, *ET SEQ.* (ON BEHALF OF PLAINTIFF ORTEGA AND THE CALIFORNIA SUBCLASS)

194. Plaintiff Ortega restates and realleges the allegations in paragraphs 1-110 as if fully set forth herein.

195. Defendants are subject to the CMIA because they are "business[es] organized for the purpose of maintaining medical information . . . in order to make the information available to an individual or provider of health care . . ." under Cal. Civ. Code § 56.06.

196. Plaintiff Ortega is a "[p]atient" as that term is defined in Cal. Civ. Code § 56.05(k). California Subclass Members are also patients under that provision.

197. As a direct result of Defendants' unlawful actions and inactions, they disclosed "medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization" by allowing third-party criminal hackers to access and exfiltrate

Plaintiffs' and California Subclass Members' PHI in violation of Cal. Civ. Code § 56.10(a).

198. Defendants breached the confidentiality of Plaintiffs' and Class Members' PHI in violation of Cal. Civ. Code § 56.101(a) by allowing unauthorized individuals to access Plaintiffs' and California Subclass Members' PHI.

199. Plaintiff Ortega and California Subclass Members have suffered actual injury and are entitled to damages under Cal. Civ. Code §§ 56.35 and 56.36 in an amount to be proven at trial.

COUNT IX
VIOLATION OF THE CLRA, CAL. CIV. CODE § 1750, *ET SEQ.* (ON BEHALF OF PLAINTIFF ORTEGA AND THE CALIFORNIA SUBCLASS)

200. Plaintiff Ortega restates and realleges the allegations in paragraphs 1-110 as if fully set forth herein.

201. Plaintiff Ortega and California Subclass Members are "consumers" as the term is defined by California Civil Code § 1761(d).

202. Plaintiff Ortega and California Subclass Members have engaged in "transactions" with Defendants, as that term is defined by California Civil Code § 1761(e).

203. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." Defendants violated this provision by representing to Plaintiff Ortega and California Subclass Members that they would take appropriate measures to protect Plaintiff Ortega's and California Subclass Members' Private Information.

204. Based on Defendants' representations, Plaintiff Ortega and California Subclass members were induced to enter into a business relationship with Defendants and provide their PII and PHI.

205. As a result of engaging in such conduct, Defendants have violated Cal. Civ. Code § 1770.

206. Pursuant to Cal. Civ. Code §§ 1780(a)(2) and (a)(5), Plaintiff Orega seeks an order of this Court that enjoins Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law. Plaintiff Ortega and California Subclass Members may be irreparably harmed and denied an effective and complete remedy if such an order is not granted.

COUNT X
VIOLATION OF THE ACFA, ARIZ. REV. STAT. § 44-1521, *ET SEQ.* (ON BEHALF OF PLAINTIFF COLE AND THE ARIZONA SUBCLASS)

207. Plaintiff Cole restates and realleges the allegations in paragraphs 1-110 as if fully set forth herein.

208. The ACFA provides that "[t]he act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

209. Plaintiff Cole and Arizona Subclass Members are "person[s]" as defined in Ariz. Rev. Stat. § 44-1521(6).

210. Defendants APC and AZPC (the "Arizona Defendants") are involved in the "sale" of "merchandise" as those terms are defined in Ariz. Rev. Stat. §§ 44-1521(5) and 1521(7).

211. The Arizona Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the "sale" and "advertisement" of "merchandise"

(as those terms are defined in the ACFA) in violation of the ACFA, Ariz. Rev. Stat. § 44-1522(A) including but not limited to the following:

a. failing to maintain sufficient security to keep Plaintiff Cole's and Arizona Class Members' confidential medical, financial, and personal data from being hacked and stolen;

b. misrepresenting material facts to Plaintiff Cole and Arizona Class Members in connection with the sale of health benefits services by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Arizona Class Members' PHI from unauthorized disclosure, release, data breaches, and theft;

c. misrepresenting material facts to Arizona Class Members in connection with the sale of medical services by representing that the Arizona Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Arizona Class Members' Private Information;

d. failing to disclose the Data Breach to Arizona Class Members in "the most expedient manner possible and without unreasonable delay" in violation of Ariz. Rev. Stat. § 44-7501; and

e. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Arizona Class Members' personal information from further unauthorized disclosure, release, data breaches, and theft.

212. The Arizona Defendants' failure to disclose that their computer systems were not well-protected and that Plaintiff Cole's and Arizona Class Members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because the Arizona Defendants

knew such facts would be unknown to and not easily discoverable and would defeat their patients' ordinary, foreseeable and reasonable expectations concerning the security of the Arizona Defendants' computer servers.

213. The Arizona Defendants intended that Plaintiff Cole and Arizona Class Members rely on their deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with the Arizona Defendants' provision of medical services and maintaining Plaintiff Cole's and Arizona Class Members' Private Information on their computer servers. This was a violation of the AFCA.

214. The Arizona Defendants also engaged in unfair acts and practices in connection with the sale of medical services by failing to maintain the privacy and security of Plaintiff Cole's and Arizona Class Members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws like FTCA, HIPAA, and the Arizona Insurance Information and Privacy Act, Ariz. Rev. Stat. § 20-2113, resulting in the Data Breach.

215. The Arizona Defendants' wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on their part that applied to Arizona Class Members and were repeated continuously before and after the Arizona Defendants obtained confidential medical, financial, and personal data concerning Plaintiff Cole and Arizona Class Members. Plaintiff Cole and Arizona Class Members have been adversely affected by the Arizona Defendants' conduct and the public was and is at risk as a result thereof.

216. As a result of the Arizona Defendants' wrongful conduct, Plaintiff Cole and Arizona Class Members were injured in that they never would have allowed their sensitive and personal data to be provided to the Arizona Defendants if they had known that the Arizona Defendants failed to maintain sufficient security to keep their data from being stolen.

217. The Arizona Defendants' unfair and/or deceptive conduct proximately caused Plaintiff Cole's and Arizona Class Members' injuries because, had the Arizona Defendants adequately secured their Private Information, Plaintiff Cole and Arizona Class Members would not have lost it.

218. Plaintiff Cole and Arizona Class Members seek actual damages, compensatory, punitive damages, injunctive relief, and court costs and attorneys' fees as a result of the Arizona Defendants' violations of the AFCA.

COUNT XI
INVASION OF PRIVACY
(ON BEHALF OF PLAINTIFFS AND THE CALIFORNIA AND ARIZONA SUBCLASSES)

219. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

220. Plaintiffs and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is protected from disclosure by applicable laws set forth above.

221. Defendants unlawfully invaded the privacy rights of Plaintiffs and Class Members by failing to adequately secure their PII and PHI from disclosure to unauthorized parties for improper purposes. This invasion into the privacy interest of Plaintiff and Class Members is serious and substantial.

222. In failing to adequately secure Plaintiffs' and Class Members' PII and PHI, Defendants acted in reckless disregard of Plaintiffs' and Class Members' privacy rights.

223. Defendants' disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties as a result of their failure to adequately secure and safeguard Plaintiffs' and Class Members' Private Information is offensive. Defendants' disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties permitted the physical and electronic

intrusion into private quarters where Plaintiffs' and Class Members' Private Information was stored.

224. Defendants violated Plaintiffs' and Class Members' right to privacy under the common law as well as under state law, including the California and Arizona state Constitutions. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiffs' and Class Members' reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and Class Members have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

225. Plaintiffs and Class Members have been damaged by Defendants' conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT XII
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

226. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

227. This count is pleaded in the alternative to Counts III and IV above.

228. Plaintiffs and Class Members conferred a benefit on Defendants by paying for services that should have included data and cybersecurity protection to protect their Private Information, which Plaintiffs and Class Members did not receive.

229. Defendants have retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that they did not provide. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

230. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants, and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

231. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT XIII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE CALIFORNIA AND ARIZONA SUBCLASSES)

232. Plaintiffs restate and reallege the allegations in paragraphs 1-110 as if fully set forth herein.

233. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

234. Defendants owe a duty of care to Plaintiffs and Class Members, which required Defendants to adequately secure the Private Information.

235. Defendants still possesses Private Information regarding Plaintiffs and Class Members.

236. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

237. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure its patients' Private Information under the common law and Section 5 of the FTCA;

b. Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure their patients' Private Information.

238. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect their patients' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting training and education to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating their patients about the threats they face with regard to the security of their Private Information, PII, and PHI, as well as the steps their patients must take to protect themselves.

239. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury and lack an adequate legal remedy to prevent another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If Defendant suffers another breach, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

240. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft, medical identity theft, and other related damages. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security

measures is relatively minimal, and Defendants have a preexisting legal obligation to employ such measures.

241. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach, thus preventing future injury to Plaintiffs and Class Members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

b. Judgment in favor of Plaintiffs and Class Members, awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: February 28, 2023

Respectfully submitted,

/s/Kyle McLean

SIRI & GLIMSTAD LLP
Kyle McLean (SBN 330580)
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 376-3739
E: kmclean@sirillp.com

Mason A. Barney (*pro hac vice* to be filed)
Steven D. Cohen (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: scohen@sirillp.com

Counsel for Plaintiffs and the Proposed Class